CLAIMS

What is claimed is:

Sub A3

1. A method for securely transferring data between an agent and an application server through a non-secure node comprising:

(a) establishing a session key between the agent and the application server by utilizing a public key of the application server; wherein the public key of the application server in embedded in the agent; and

(b) establishing an end-to-end secure connection between the agent and the application server by using the session key and by establishing a communication link between the application server and the non-secure node by using a relay module.

2. The method of claim 1 wherein establishing a communication link between the application server and the non-secure node by using a relay module comprises:

dynamically instantiating the relay module having a first port for communicating with the application server and a second port for communicating with the agent, the relay module listening on a first predetermined port number on the first port and a second predetermined port number on the second port; and

the application server connecting to the first port of the relay module to establish a connection therewith.

3. The method of claim 2 wherein establishing a communication link between the application server and the agent through a relay module further comprises:

pushing data encrypted by the established session key from the agent to the application server over the end-to-end secure connection.

4. The method of claim 2 wherein establishing a communication link between the application server and the agent through a relay module further comprises:

pulling data encrypted by the session key from the application server over the end-to-end secure connection to the agent.

5. The method of claim 1 wherein establishing a session key between the agent and the application server by utilizing a public key of the application server further comprises:

establishing a shared secret key between the application server and the agent for encrypting and decrypting data sent therebetween.

6. The method of claim 5 wherein establishing a shared secret key between the application server and the agent for encrypting and decrypting data sent therebetween comprises:

encrypting the shared secret key with the public key of the application server to generate an encrypted shared key;

sending the encrypted shared secret key to the application server; and

decrpyting the shared secret key with the private key of the application server.

7. The method of claim 5 wherein establishing a shared secret key between the application server and the agent utilizes a key transfer protocol.

8. The method of claim 7 wherein the key transfer protocol is the Rivest, Shamir, Adleman (RSA) public key algorithm.

9. The method of claim 5 wherein establishing a shared secret key between the application server and the agent for encrypting and decrypting data sent therebetween utilizes a key agreement protocol.

10. The method of claim 9 wherein the key agreement protocol is the Diffie-Hellman (DH) public key algorithm.

11. The method of securely transferring data between an application server and an agent of the application server through a non-secure environment having a web-server and the agent, the method comprising:

a) a user accessing the web-server to download the agent therefrom; wherein the agent includes a public key of the application server;

b) the agent establishing a shared session key with the application server by using the public key of the application server, the shared session key for use in encrypting and decrypting data to be transferred between the agent and the application server;

c) the application server establishing a connection to the web-server; and

d) the agent contacting the web server by using a first protocol to send data encrypted by the session key to the application server over the connection between the web-server and the application server.

12. The method of claim 11 wherein the application server establishing a connection to the web-server further comprises

c1) the application server dynamically instantiating a relay module by sending a URL associated with the relay module to the web-server, the URL specifying a first predetermined port for communication between the web-server and the relay module;

c2) the application server connecting to the relay module on a first predetermined port; and

c3) the application server reading data from the relay module through the connection on the first predetermined port.

13. The method of claim 12 wherein the agent contacting the web server by using a first protocol to send data encrypted by the session key to the application server over the connection between the web-server and the application server further comprises

d1) the agent encrypting the session key with the public key of the application server;

d2) the agent collecting data;

d3) the agent encrypting the collected data with the session key;

d4) sending the encrypted session key and encrypted measured data to the application server by using a forwarding module that connects to a second predetermined port of the relay module.

14. The method of claim 11 wherein the first protocol is one of HTTP and HTTP/SSL.

15. A secure data transfer system for connecting a non-secure node to an application server behind a firewall comprising:

a) a web-server in the non-secure node;

b) a relay in the non-secure node that is dynamically instantiated by the application server, the relay having a first port for listening for a connection from the application server;

wherein the application server connects to the relay on the first port and reads data from the first port.

16. The secure data transfer system of claim 15 further comprising:

a) an instantiation module for instantiating the relay module in response to an URL associated with the relay module.

17. A secure data transfer system for establishing an end-to-end secure connection between an agent and an application server behind a firewall through a non-secure node comprising:

a) a web-server residing in the non-secure node, the web-server having the agent that includes a public key of the application server;

b) a browser in communication with the web-server for downloading the agent from the web-server;

c) a secure transfer module residing in the non-secure node; and

d) an application server in a secure zone for initiating a connection to the web-server via the secure transfer module.

18. The secure data transfer system of claim 17 wherein the secure transfer module further comprises:

c1) a relay module for listening to a first port and a second port;

c2) an instantiation module for executing the relay module in response to a command from the application server;

c3) a forwarding module for transferring data from the agent to the relay module in response to a command from the agent; and

wherein the relay module listens to the first port for a connection by the application server and listens to the second port for a connection by the forwarding module.

19. The secure data transfer system of claim 16 wherein the non-secure node is a web-server node.